A brief response to *Strengthening Australia's Cyber Ssecurity Regulations and Incentives: An initiative of Australia's Cyber Security Strategy 2020*

School of Computer Science, Faculty of Science, The Queensland University of Technology (compiled by Prof. Raja Jurdak, https://staff.qut.edu.au/staff/r.jurdak)

We thank the Federal Government for its timely circulation of this discussion paper, whose observations are already influencing research proposals currently being developed at the Queensland University of Technology.

With respect to the specific discussion points listed in Appendix A (pages 58 and 59), we make the following observations.

1. The lack of sufficient cybersecurity standards and regulations, as well as systems and incentives that enable automated detection, assessment, and sharing of threats are some of the factors that limit the adoption of cybersecurity best practice in Australia.

2. Negative externalities and information asymmetries do create a need for Government action on cybersecurity. Specifically, there is a need for Government to step in with regulation and a framework for risk sharing of cybersecurity threats, whereby the negative impacts of suppliers or customers of an entity that experiences a cybersecurity attack are shared by that entity if it is confirmed not to have implemented the required cybersecurity protections.

5. The best approach to strengthening corporate governance of cybersecurity risk would be a combination of a voluntary governance standard, with a highly transparent system (such as a cybersecurity rating system) that reflects the degree of rigour in cybersecurity governance measures adopted by a commercial entity.

11. Strengthening the cybersecurity of smart devices in Australia would benefit from minimum standards and a secure registry of identified vulnerabilities that is accessible to authenticated and authorised entities for more timely responses to the identified vulnerabilities.

16. A dynamic security rating system would work best for encouraging secure smart devices. A static physical rating with an expiry date would work well for initial purchases, but a dynamic and easily accessible digital rating based on the current firmware/updates for the device could maintain more current security ratings and encourage consumers to update software with patches regularly.

19. An expiry date for security is not ideal without linking to regular updates and more dynamic information. Cyberthreats are fast moving and an initial static expiry date may become obsolete if new unexpected threats arise.

20. A mandatory scheme should include mobile phones, as they are sensor and data rich devices with significant security and privacy risks.

21. Labels should be both physical and digital, with the physical label characterising the initial security rating of the device and the digital label providing a more dynamic and up-to-date rating.

22. There is potential to link the security star rating of a supplier/device to the extent of identified vulnerabilities/threats by that supplier/device, which can incentivise threat identification through better ratings.